

CLAIMS

1 1. A computer authentication protocol, comprising:

2 sending at least one certificate payload from a transmitting computer
3 to a receiving computer, the certificate payload including at least two
4 certificates each being generated by a respective certificate authority (CA), the
5 certificate authorities being independent of each other such that no trust
6 relationship exists between the CA.

1 2. The protocol of claim 1, wherein the certificates are concatenated
2 together.

1 3. The protocol of Claim 2, wherein at least one certificate is associated
2 with a person and one certificate is associated with a host computer.

1 4. The protocol of Claim 1, further comprising sending at least one
2 identification (ID) payload between the computers, the ID payload being generated by
3 combining the IDs of at least two entities.

1 5. The protocol of Claim 4, further comprising sending at least one
2 signature payload between the computers, the signature payload being generated by
3 concatenating the signatures of at least two entities.

1 6. The protocol of Claim 4, wherein each signature is formed by applying
2 a pseudorandom function (PRF) to at least the associated ID to render a result, and
3 then encrypting the result with a private key associated with the entity represented by
4 the ID.

1 7. A computer program device, comprising:
2 a computer program storage device including a program of instructions
3 usable by a computer, comprising:
4 logic means for combining a first entity identification (ID) with a
5 second entity ID to render an ID payload; and
6 logic means for sending the ID payload to a computer along with at
7 least one certificate payload.

1 8. The computer program device of Claim 7, further comprising:
2 logic means for generating a signature payload by concatenating at least
3 two signatures of respective entities.

1 9. The computer program device of Claim 8, wherein the means for
2 generating a signature payload applies a pseudorandom function (PRF) to at least an
3 ID associated with an entity to render a result, and then encrypting the result with a
4 private key associated with the entity represented by the respective ID.

1 10. A computer program device, comprising:
2 a computer program storage device including a program of instructions
3 usable by a computer, comprising:
4 logic means for generating a signature payload by concatenating at least
5 two signatures of respective entities; and
6 logic means for sending the signature payload to a computer along with
7 at least one certificate payload.

1 11. The computer program device of Claim 10, wherein the means for
2 generating a signature payload applies a pseudorandom function (PRF) to at least an
3 ID associated with an entity to render a result, and then encrypting the result with a
4 private key associated with the entity represented by the respective ID.

1 12. The computer program device of Claim 11, further comprising:
2 logic means for combining a first entity ID with a second entity ID to
3 render an ID payload; and
4 logic means for sending the ID payload to a computer along with at
5 least one certificate payload.

1 13. A computer system for secure network authentication, comprising:

2 at least one host certificate authority (CA) generating a host
3 authentication certificate for at least one host computer; and
4 at least one user CA generating a user authentication certificate for at
5 least one user, wherein the certificates can be combined into a certificate
6 payload during an authentication process, the host CA not being in a trust
7 relationship with the user CA and vice-versa.

1 14. The system of claim 13, wherein the certificates are concatenated
2 together to establish a certificate payload.

1 15. The system of Claim 14, wherein at least one certificate is associated
2 with a person and one certificate is associated with a host computer.

1 16. The system of Claim 13, wherein the system sends at least one
2 identification (ID) payload between the computers, the ID payload being generated by
3 combining the IDs of at least two entities.

1 17. The system of Claim 16, wherein the system sends at least one
2 signature payload between the computers, the signature payload being generated by
3 concatenating the signatures of at least two entities.

1 18. The system of Claim 17, wherein each signature is formed by applying
2 a pseudorandom function (PRF) to at least the associated ID to render a result, and
3 then encrypting the result with a private key associated with the entity represented by
4 the ID.